Abstract

Techniques for providing secure communications between two or more end units of a call processing system via a call complex or other communication system switch. The end units each generate a set of session key lists including a stack-based session key list for each of the terminals coupled thereto. The multiple sets of session key lists are communicated from the end units to the call complex in a secure manner as part of corresponding authentication protocols carried out between the end units and the call complex. In establishing secure communications between an originating end unit and one or more additional end units, the call complex selects, as an end unit to end unit session key, a session key from a session key list in a given one of the sets of session key lists associated with the originating end unit. The selected end unit to end unit session key is used to provide secure communications between the originating end unit and at least one other end unit via the call complex. The same end unit to end unit session key is preferably used for any additional end units subsequently conferenced into the secure communication channel between the originating end unit and a specified destination end unit. Upon termination of the secure communication channel, one or more new session keys can be generated for the affected terminals so as to maintain a desired minimum stack size for the session key lists.